

# UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Information Associated with  
deloveamuzu98@yahoo.com That is Stored at Premises  
Controlled by Oath Holdings Inc.

Case No. **1:21-MJ-00718**

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A (incorporated by reference).

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1341	Mail Fraud

The application is based on these facts:

See Attached Affidavit (incorporated by reference).

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

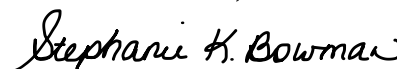
  
Applicant's signature

Aaron Bauder, FBI Special Agent  
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
FaceTime Video Conference (specify reliable electronic means).

Date: Oct 8, 2021

City and state: Cincinnati, Ohio

  
Judge's signature

Hon. Stephanie K. Bowman, U.S. Magistrate Judge

Printed name and title



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with  
DELOVEAMUZU98@YAHOO.COM that is stored at premises owned, maintained, controlled,  
or operated by Oath Holdings Inc. (“Oath”), a company headquartered at 701 First Avenue,  
Sunnyvale, CA 94089.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Oath (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 9, 2021, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account from **January 28, 2017, to present**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud) and 1341 (Mail Fraud), those violations involving DELOVE KOFI AMUZU and occurring after in or about January 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) A “romance fraud” scheme;
- (b) Evidence of false misrepresentations made to victims designed to induce those victims to send money to accounts controlled by AMUZU and/or any coconspirators;
- (c) The identities of any coconspirators of AMUZU;
- (d) The receipt and disposition of funds from victims of a “romance fraud” scheme;
- (e) Financial accounts, social media accounts, online dating accounts, and other online accounts used by the user of the Account;
- (f) Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (g) Evidence indicating the Account owner’s state of mind as it relates to the crime under investigation;
- (h) The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).
- (i) The identity of the person(s) who communicated with the Account about matters relating to the Target Offenses, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
DELOVEAMUZU98@YAHOO.COM THAT  
IS STORED AT PREMISES CONTROLLED  
BY OATH HOLDINGS INC.

Case No. 1:21-MJ-00718

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Aaron Bauder, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with **DELOVEAMUZU98@YAHOO.COM** (the “**SUBJECT ACCOUNT**”) that is stored at premises controlled by Oath Holdings Inc. (“Oath”), an email provider headquartered at 701 First Avenue, Sunnyvale, CA 94089. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Oath to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been employed as a Special Agent with the FBI since 2019 and am currently assigned to the White Collar Crimes Squad of the Cincinnati Field Office. In this capacity, I investigate white collar crimes, including civil rights violations, money laundering, and various types of fraud. Since 2019, I have received training and experience in interview and interrogation techniques, arrest procedures, search warrants, and various other investigative

techniques. As an FBI Special Agent, I am responsible for enforcing, and for investigating violations of, United States laws dealing with financial fraud, including violations of 18 U.S.C. § 1343 (Wire Fraud).

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that DELOVE KOFI AMUZU has violated 18 U.S.C. §§ 1341 (Wire Fraud) and 1343 (Mail Fraud). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

#### **A. Introduction and Background on “Romance Fraud” Schemes**

6. The FBI and the U.S. Attorney’s Office for the Southern District of Ohio are investigating a suspected “romance fraud” scheme being perpetrated by DELOVE KOFI AMUZU, and others known and unknown.

7. Based on my training and experience, I know the following about romance fraud schemes:



- a. Perpetrators of romance fraud schemes commonly create false profiles on dating websites using false information and stolen pictures of individuals. In this Affidavit, I will call these imaginary attractive individuals the "Romantic Partner(s)."
- b. The perpetrators use the false online profiles to initiate contact with victims. Once the perpetrators have initiated contact with a victim, pretending to be a Romantic Partner, they communicate with the victim primarily by messaging services. By expressing romantic interest in the victim, the perpetrators mislead the victim into believing he or she is in a relationship with the Romantic Partner.
- c. The perpetrators commonly represent that the Romantic Partner is currently abroad, providing a justification as to why the Romantic Partner is never able to meet the victim in person.
- d. Once the victim believes he or she is in a romantic relationship with the Romantic Partner, the perpetrators begin asking the victim to send money and/or other items of value. Commonly, the Romantic Partner falsely represents that he or she is expecting a large inheritance of gold bars and is seeking to bring the gold bars to the United States. The Romantic Partner induces the victim to send money to pay for expenses associated with the gold inheritance. Other false representations that Romantic Partners commonly make are that they need money for a plane ticket to visit the victim, money for bail after being falsely imprisoned, or money to pay medical bills. In fact, the money and valuables the victims send to the perpetrators are used for other purposes.

8. As I explain in more detail below, based on the investigation to date, as well as my training and experience investigating romance fraud schemes, there is probable cause to

believe that AMUZU is perpetrating a romance fraud scheme involving violations of 18 U.S.C. §§ 1343 and 1341 and that the **SUBJECT ACCOUNT** described in Attachment A will contain evidence, instrumentalities, fruits, and contraband of those violations, as described in Attachment B.

**B. In 2018, VICTIM 1 developed an online romantic relationship with someone calling himself “Marvin Anderson,” who directed VICTIM 1 to send him thousands of dollars.**

9. I interviewed VICTIM 1 in March 2020. VICTIM 1 told me that, in approximately April 2018, VICTIM 1 met an individual online who called himself “Marvin Anderson.” After speaking with Anderson by phone and email, VICTIM 1 developed what she believed was a romantic relationship with Anderson.

10. VICTIM 1 said Anderson spoke with a foreign accent. VICTIM 1 said Anderson claimed to live near VICTIM 1 but said he was working on a construction project in Egypt.

11. At some point, Anderson said he and his daughter were traveling to Egypt, and he asked VICTIM 1 to send money to assist with their travel costs, which VICTIM 1 did. VICTIM 1 estimated that, in total, she had sent Anderson approximately \$75,000.

12. VICTIM 1 said that, in August 2018, she told Anderson that if he wanted to continue their relationship, he would have to meet her in person. Anderson declined, and the relationship ended.

**C. Shortly after breaking up with “Anderson,” VICTIM 1 developed met “Dion Wilson,” who directed her to send valuables to AMUZU.**

13. VICTIM 1 said that, later in August 2018, shortly after breaking up with “Anderson,” VICTIM 1 met an individual online who went by the name “Dion Wilson.” VICTIM 1 said that Wilson, like Anderson, spoke with a foreign accent.

14. Wilson told VICTIM 1 he knew two FBI agents in Egypt who could assist VICTIM 1 in finding Anderson and retrieving her money. Wilson put VICTIM 1 in touch with one of the alleged FBI agents, "Carol." VICTIM 1 said that, at Carol's request, VICTIM 1 had sent Carol \$25,000 to begin looking for Anderson.

15. VICTIM 1 said that Wilson then introduced her to "Nelson Meeks," an individual he said was his banker. Wilson told VICTIM 1 Meeks would handle the financial side of the investigation. VICTIM 1 said that, when she spoke with Meeks by phone, he also had a foreign accent.

16. VICTIM 1 shared her bank information with Meeks, and between September and November of 2018, she noticed money being stolen from her accounts and from her home equity loan. When she addressed the issue with Wilson, he blamed Meeks for "stealing from us."

17. VICTIM 1 said Wilson also asked her to purchase items for what he described as his coffee bean business, "Evergreen." VICTIM 1 said Wilson had provided a link to a website with a video about the company and had shown her information showing that Evergreen's bank account contained \$23 million.

18. At Wilson's direction, VICTIM 1 purchased several items, such as computers, iPhones, iPads, laptops, and Rolex watches, and mailed these items to AMUZU in Cincinnati, Ohio. VICTIM 1 never spoke directly with AMUZU, but Wilson told VICTIM 1 that AMUZU was in the process of purchasing Evergreen.

**D. Wilson also directed VICTIM 1 to send money to accounts controlled by AMUZU, allegedly to assist with the sale of Evergreen to AMUZU.**

19. VICTIM 1 said that, at Wilson's direction, she also sent money to accounts in the name of Obdomdel Management Agency LLC, an LLC whose registered agent is (and at the time was) AMUZU.

20. Records from VICTIM 1's financial accounts show that on November 8, 2018, a wire transfer for \$97,000 cleared from VICTIM 1's account at Canvas Credit Union to an account at Bank of America in the name of Obdomdel Management Agency LLC, with an account number ending in 9130 ("Bank of America Account 9130"). At the time of the transaction, AMUZU was listed as the sole owner/signer on Bank of America Account 9130.

21. Bank records also show that, the next day, November 9, 2018, a wire transfer for \$85,000 cleared from Obdomdel Management Agency LLC's Bank of America Account 9130 account to a bank account in Ghana (AMUZU's home country). The subject line for the wire said, "PURCHASE OF HOUSE."

22. Bank records also show that on November 10, 2018, VICTIM 1 sent a cashier's check from Canvas Credit Union, payable to Obdomdel Management Agency LLC (AMUZU's LLC), for \$101,000. On November 13, 2018, the check cleared to an account in the name of Obdomdel Management LLC, with an account number ending in 8163, at Wells Fargo Bank ("Wells Fargo Account 8163"). As of that date, AMUZU was the sole owner and signer on Wells Fargo Account 8163.

- E. VICTIM 2 began a romantic relationship online with “Christian Coleman,” who directed VICTIM 2 to send money to accounts controlled by AMUZU.**

23. Steve Isgro, an Investigator for the Butler County Prosecutor’s Office, interviewed VICTIM 2 in April and October 2019. FBI Special Agent Ferron Yi interviewed VICTIM 2 again via telephone in May 2020.

24. VICTIM 2 said that, in approximately 2017, she met an individual who called himself “Christian Coleman” on the online dating website “Plenty of Fish,” and the two developed a romantic relationship. VICTIM 2 said Coleman had spelled his name several different ways over the course of their communications.

25. VICTIM 2 said Coleman claimed to be an engineer who was on an extended trip overseas. Coleman led VICTIM 2 to believe that he had attempted to return to the United States several times during their relationship, but he always had an excuse as to why he had to remain overseas.

26. VICTIM 2 said that, on Coleman’s behalf, she had accepted tens of thousands of dollars from other individuals.

27. VICTIM 2 said that, at Coleman’s direction, she had worked with Nelson Meeks—same person “Dion Wilson” told VICTIM 1 was his banker—to transfer money and valuables.

28. According to VICTIM 2, Coleman eventually said he was inheriting gold from his father and asked VICTIM 2 to send money and valuables to him to assist with the acquisition of the gold.

29. VICTIM 2 said that, at some point, Coleman told VICTIM 2 he wanted to come back to the United States to start a new business. He explained to VICTIM 2 that he had multiple

investors lined up and would need additional funding from her. Coleman then connected her to an individual who lived in Fairfield, Ohio, who Coleman said would receive money from her on Coleman's behalf. (As of May 2020, VICTIM 2 could not remember the name of the person living in Fairfield, Ohio; however, AMUZU was associated with an address in Fairfield, Ohio, as of 2018, and, as I explain below, bank records show that VICTIM 2 sent money to accounts controlled by AMUZU, including an account in his name.)

30. Bank records show that, in November 2018, VICTIM 2 sent approximately \$72,300 to Obdomdel Management Agency LLC and to bank accounts in AMUZU's name. Specifically, on November 26, 2018, a counter deposit for \$36,500, drawn from VICTIM 2's account at PNC Bank, cleared to an account in AMUZU's name at BB&T Bank ("BB&T Account 7112"). Shortly thereafter, on November 30, 2018, a wire transfer for \$35,800 from VICTIM 2's PNC Bank account cleared to Obdomdel Management LLC's Bank of America Account 9130.

**F. VICTIM 3 began an online romantic relationship with "Hannah Arthur," who directed him to send money and valuables to AMUZU, allegedly to help her pay taxes on millions of dollars in gold she was inheriting.**

31. On November 10, 2020, FBI Special Agent Timothy J. Ervin interviewed VICTIM 3. I have reviewed SA Ervin's interview report, as well as supporting documentation provided by VICTIM 3's daughter.

32. VICTIM 3 said that, in March 2020, he met an individual using the name "Hannah Arthur" (hereafter "Hannah") on a dating website called "Rendezvous." Although VICTIM 3 had never met Hannah in person, by exchanging messages on WhatsApp and Google Hangouts VICTIM 3 and Hannah developed what VICTIM 3 believed was a romantic relationship. VICTIM 3 said Hannah had an American accent.

33. VICTIM 3 said that Hannah told him she was a student in Ghana who had just inherited \$8,500,000 in gold bars and other various currencies. Hannah asked VICTIM 3 to send money to pay the taxes, fees, and tariffs necessary to release the gold bars.

34. VICTIM 3 said Hannah had directed him to send cashier's checks to several individuals to get the gold bars released. VICTIM 3 said that, among the people to whom Hannah directed VICTIM 3 to send money was AMUZU, at three different addresses in Ohio.

35. VICTIM 3 said that Hannah had also directed him to send multiple cell phones to AMUZU at an address in Bronx, New York.

36. VICTIM 3's daughter provided a spreadsheet showing payments and shipments VICTIM 3 had made at Hannah's direction. Among the payments and shipments listed were the following:

Date	Amount / Items	Recipient Account or Mail-to Address
7/17/2020	\$60,376.00 cashier's check deposit	[another known victim, G.H.]
7/30/2020	\$101,000.00 cashier's check deposit	[G.H.]
8/14/2020	\$26,500.00 cash deposit	Delove Kofi Amuzu [Redacted], Fairfield, OH 45104
9/12/2020	\$65,000.00 cashier's check deposit	Delove Kofi Amuzu, [Redacted], Cincinnati, OH 45251
10/9/2020	16 iPhones	Delove Kofi Amuzu, [Redacted], Bronx, NY 10452

37. Bank records show that on August 14, 2020, a counter deposit for \$26,500 cleared to an account at BB&T with an account number ending in 1162 ("BB&T Account 1162"). This payment corresponds to one that VICTIM 3's daughter's spreadsheet lists as a "Cash Deposit"



made by VICTIM 3 on August 14, 2020. As of August 14, 2020, AMUZU was the sole owner of and signer on BB&T Account 1162.

38. Bank records also show that on September 14, 2020, a counter deposit from VICTIM 3's Wells Fargo cashier's check #6888903115, for \$65,000, cleared to AMUZU's BB&T Account 1162. This payment appears to correspond to another payment that VICTIM 3's daughter's spreadsheet lists as a "cashier's check deposit," which VICTIM 3 made on September 12, 2020.

**G. In 2018, VICTIM 4 began an online romantic relationship with "Noel Hernandez" and was directed to send money to AMUZU's PayPal account.**

39. In November 2018, VICTIM 4 submitted an IC3 Complaint in which he claimed to have been the victim of a romance fraud scheme involving AMUZU.

40. In April 2020, FBI SA Michael Reigle interviewed VICTIM 4, who explained that in September 2018 he had gotten into an online relationship with "Noel Hernandez," who claimed to be a sergeant in the U.S. Army. According to VICTIM 4, Hernandez originally claimed to be stationed in London but later claimed she had moved to Africa. Hernandez told VICTIM 4 she could not provide specifics as to her location for security reasons.

41. Eventually, Hernandez told VICTIM 4 that she had an inheritance coming to her in the form of gold and diamonds but that the gold had gotten "hung up" in customs. Hernandez told VICTIM 4 that she needed money to get the gold released. VICTIM 4 explained that, at Hernandez's direction, he ended up sending money to five different locations, for a total of approximately \$150,000 in loss.



42. VICTIM 4 said he was directed to send money to DELOVE AMUZU via PayPal. In his IC3 Complaint, VICTIM 4 said AMUZU's email address was **DELOVEAMUZU98@YAHOO.COM** (i.e., **THE SUBJECT ACCOUNT**).

43. I reviewed financial records showing that on November 9, 2018, VICTIM 4 sent three payments via PayPal, totaling \$12,000, to a PayPal account in the name of DE LOVE AMUZU.

44. Bank records also show that on October 30, 2018, and November 2, 2018, VICTIM 4 wired \$4,000 and \$10,000, respectively, to an account in the name of Obdomdel Management LLC (on which account AMUZU was then the sole signer). The memo line on both transfers was "Securities/[VICTIM 4's last name]/Hernandez."

**H. The subscriber email address for AMUZU's PayPal account is the SUBJECT ACCOUNT.**

45. Records from PayPal show that the PayPal account in AMUZU's name is associated with AMUZU's addresses in Fairfield, OH, and in Bronx, NY. The PayPal account is also linked to several bank accounts and debit cards in AMUZU's name.

46. Records from PayPal further show that, consistent with VICTIM 4's IC3 Complaint, the subscriber email address associated with AMUZU's PayPal account is the **SUBJECT ACCOUNT**. The PayPal records further indicate that, as of February 2021, the **SUBJECT ACCOUNT** was "confirmed" and "active."

**I. Records from Oath provide further evidence that the SUBJECT ACCOUNT is used by AMUZU.**

47. Records from Oath show that the **SUBJECT ACCOUNT** has a subscriber name of "Delove amuzu." The account was opened on January 28, 2017.

48. The Google records show that the **SUBJECT ACCOUNT** was most recently logged into on July 21, 2021.

49. The verified recovery telephone number for the **SUBJECT ACCOUNT** is 347-554-4344. Records from US Bank show that on February 28, 2018, AMUZU opened a bank account with an account number ending in 6002, listing his primary telephone number as 347-554-4344.

50. On September 9, 2021, I sent a preservation request to Oath, requesting that it preserve records associated with the **SUBJECT ACCOUNT** for 90 days. In general, an email that is sent to an Oath subscriber is stored in the subscriber's "mail box" on Oath's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Oath's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Oath's servers for a certain period of time.

#### **BACKGROUND CONCERNING EMAIL**

51. In my training and experience, I have learned that Oath provides a variety of on-line services, including electronic mail ("email") access, to the public. Oath allows subscribers to obtain email accounts at the domain name yahoo.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Oath. During the registration process, Oath asks subscribers to provide basic personal information. Therefore, the computers of Oath are likely to contain stored electronic communications (including retrieved and unretrieved email for Oath subscribers) and information concerning subscribers and their use of Oath services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute

evidence of the crimes under investigation because the information can be used to identify the account's user or users.

52. An Oath subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Oath. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

53. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

54. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address

("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

55. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

56. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol

(IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

### **CONCLUSION**

57. Based on the foregoing, I request that the Court issue the proposed search warrant.

58. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Oath. Because the warrant will be served on Oath, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

### **REQUEST FOR SEALING**

59. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These

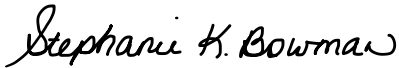
documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



AARON BAUDER  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to via FaceTime videoconference on October 8, 2021.



Honorable Stephanie K. Bowman  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with  
DELOVEAMUZU98@YAHOO.COM that is stored at premises owned, maintained, controlled,  
or operated by Oath Holdings Inc. ("Oath"), a company headquartered at 701 First Avenue,  
Sunnyvale, CA 94089.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Oath (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 9, 2021, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account from **January 28, 2017, to present**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and



e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud) and 1341 (Mail Fraud), those violations involving DELOVE KOFI AMUZU and occurring after in or about January 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) A “romance fraud” scheme;
- (b) Evidence of false misrepresentations made to victims designed to induce those victims to send money to accounts controlled by AMUZU and/or any coconspirators;
- (c) The identities of any coconspirators of AMUZU;
- (d) The receipt and disposition of funds from victims of a “romance fraud” scheme;
- (e) Financial accounts, social media accounts, online dating accounts, and other online accounts used by the user of the Account;
- (f) Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (g) Evidence indicating the Account owner’s state of mind as it relates to the crime under investigation;
- (h) The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).
- (i) The identity of the person(s) who communicated with the Account about matters relating to the Target Offenses, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.